PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-044988
(43)Date of publication of application : 16.02.2001

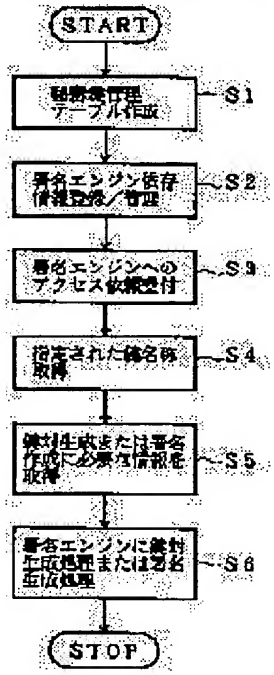
(51)Int.CI. H04L 9/32
G09C 1/00

(21)Application number : 11-221413
(22)Date of filing : 04.08.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HASHIMOTO SHOICHI
NAKAHARA SHINICHI

(54) METHOD AND SYSTEM FOR ACCESSING TO DIFFERENT SIGNATURE ENGINES IN COMMON AND STORAGE MEDIUM STORED WITH ACCESS PROGRAM TO DIFFERENT SIGNATURE ENGIENS IN COMMON

(57)Abstract:
PROBLEM TO BE SOLVED: To discriminatingly use signature engines and multiple signature algorithm with ease and to easily add a new signature engine or new signature algorithm to an existent system in such a case without affecting a higher-order application.
SOLUTION: A secret key management table which manages pieces of secret key information is generated (S1). Signature engine dependency information depending upon a signature engine is registered and managed (S2). A request to access a signature engine is accepted (S3). A specified key name is obtained (S4). Information needed for signature generation or key couple generation corresponding to the key name is obtained from the secret key management table (S5). An arbitrary signature engine is requested to generate a key couple or signature (S6).



LEGAL STATUS

[Date of request for examination] 19.10.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－44988
（P2001－44988A）
(43)公開日　平成13年２月16日(2001.2.16)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　９Ａ００１

審査請求　未請求　請求項の数12　ＯＬ　（全 18 頁）

(21)出願番号　特願平11－221413

(22)出願日　平成11年８月４日(1999.8.4)

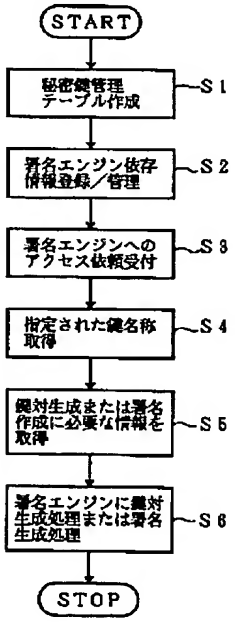
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　橋本　正一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中原　慎一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

Ｆターム(参考)　5J104 AA09 LA03 LA06 MA02 NA02
NA12 NA20 NA27
9A001 EE03 JZ64 KZ58 LL03

(54)【発明の名称】　複数の異なる署名エンジンに対する共通的なアクセス方法及びシステム及び複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体

(57)【要約】
【課題】　複数の署名エンジン及び複数の署名アルゴリズムを容易に使い分けることを可能とし、また、既存のシステムへの新たな署名エンジンの追加や新たな署名アルゴリズムの追加の際にも、上位のアプリケーションに影響を与えることなく容易に追加を行うことが可能な複数の異なる署名エンジンに対する共通的なアクセス方法及びシステム及び複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体を提供する。
【解決手段】　本発明は、複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成し、署名エンジンに依存した署名エンジン依存情報を登録し、管理し、署名エンジンへのアクセス依頼を受け付け、指定された鍵名称を取得し、秘密鍵管理テーブルから鍵名称に対応する署名作成または、鍵対生成に必要な情報を取得し、任意の署名エンジンに対して鍵対生成処理または、署名作成処理をを依頼する。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】　平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセス方法において、

複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成し、

署名エンジンに依存した署名エンジン依存情報を登録し、管理し、

前記署名エンジンへのアクセス依頼を受け付け、

指定された鍵名称を取得し、

前記秘密鍵管理テーブルから前記鍵名称に対応する鍵対生成または、署名作成に必要な情報を取得し、

任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼することを特徴とする複数の異なる署名エンジンに対する共通的なアクセス方法。

【請求項２】　前記秘密鍵管理テーブルから、前記鍵名称に対応する署名作成に必要な情報として、

前記鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得し、

取得した前記署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を前記署名エンジン依存情報から取得し、

ハッシュ化が必要な場合には、前記秘密管理テーブルから取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して前記署名エンジンへ送付し、署名生成依頼を行う請求項１記載の複数の異なる署名エンジンに対する共通的なアクセス方法。

【請求項３】　前記鍵対を生成する際に、

利用者が指定した鍵名称を取得し、

前記秘密鍵管理テーブルから前記鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得し、

取得した前記署名エンジン種別に対応するアクセスモジュール種別情報を前記署名エンジン依存情報から取得し、

前記鍵格納場所、前記署名アルゴリズム、及び前記鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼し、

前記署名エンジンにおいて、依頼された鍵対を生成する請求項１記載の複数の異なる署名エンジンに対する共通的なアクセス方法。

【請求項４】　前記利用者が指定する前記鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを、前記秘密鍵管理テーブルに保持する請求項２または、３記載の複数の異なる署名エンジンに対する共通的なアクセス方法。

【請求項５】　平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセスシステムであって、

複数の秘密鍵の管理や複数の電子署名アルゴリズムの利用が可能な任意の数の電子署名エンジンと、

複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成する秘密鍵管理テーブル作成手段と、

署名エンジンに依存した情報である署名エンジン依存情報を登録し、管理する署名エンジン依存情報登録手段と、

前記署名エンジンへのアクセス依頼を受け付け、指定された鍵名称を取得する署名エンジンアクセス依頼受付手段と、

前記秘密鍵管理テーブルから前記鍵名称に対応する秘密鍵情報及び、署名作成に必要な情報を取得する秘密鍵情報参照手段と、

任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼する署名エンジンアクセス制御手段とを有することを特徴とする複数の異なる署名エンジンに対する共通的なアクセスシステム。

【請求項６】　前記秘密鍵情報参照手段は、

前記秘密鍵管理テーブルから、前記鍵名称に対応する署名作成に必要な情報として、該鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得する手段を有し、前記署名エンジンアクセス制御手段は、

取得した前記署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を署名エンジン依存情報から取得する手段と、

ハッシュ化が必要な場合には、前記秘密管理テーブルから取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して前記署名エンジンへ送付し、署名生成依頼を行う手段を有する請求項５記載の複数の異なる署名エンジンに対する共通的なアクセスシステム。

【請求項７】　利用者が指定した鍵名称を取得する手段と、

前記秘密鍵管理テーブルから前記鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得する手段と、

取得した前記署名エンジン種別に対応するアクセスモジュール種別情報を前記署名エンジン依存情報から取得する手段と、

前記鍵格納場所、前記署名アルゴリズム、及び前記鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼する手段とを有する鍵対生成依頼手段を更に有し、

前記署名エンジンにおいて、依頼された鍵対を生成する請求項５記載の複数の異なる署名エンジンに対する共通的なアクセスシステム。

【請求項８】　前記秘密鍵管理テーブルは、

前記利用者が指定する前記鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを保持する請求項６または、７記載の複数の異なる署名エンジンに対する共通的なアクセスシステム。

【請求項９】　平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体であって、

複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成する秘密鍵管理テーブル作成プロセスと、

複数の秘密鍵の管理や複数の電子署名アルゴリズムの利用が可能な任意の数の電子署名エンジンに依存した情報である署名エンジン依存情報を登録し、管理する署名エンジン依存情報登録プロセスと、

前記署名エンジンへのアクセス依頼を受け付け、指定された鍵名称を取得する署名エンジンアクセス依頼受付プロセスと、

前記秘密鍵管理テーブルから前記鍵名称に対応する秘密鍵情報及び、署名作成に必要な情報を取得する秘密鍵情報参照プロセスと、

任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼する署名エンジンアクセス制御プロセスとを有することを特徴とする複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体。

【請求項１０】　前記秘密鍵情報参照プロセスは、

前記秘密鍵管理テーブルから、前記鍵名称に対応する署名作成に必要な情報として、該鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得するプロセスを有し、

前記署名エンジンアクセス制御プロセスは、

取得した前記署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を署名エンジン依存情報から取得するプロセスと、

ハッシュ化が必要な場合には、前記秘密管理テーブルから取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して前記署名エンジンへ送付し、署名生成依頼を行うプロセスを有する請求項９記載の複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体。

【請求項１１】　利用者が指定した鍵名称を取得するプロセスと、

前記秘密鍵管理テーブルから前記鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得するプロセスと、

取得した前記署名エンジン種別に対応するアクセスモジュール種別情報を前記署名エンジン依存情報から取得するプロセスと、

前記鍵格納場所、前記署名アルゴリズム、及び前記鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼するプロセスとを有する鍵対生成依頼プロセスを更に有する請求項９記載の複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体。

【請求項１２】　前記利用者が指定する前記鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを保持する前記秘密鍵管理テーブルを利用するプロセスを有する請求項１０または、１１記載の複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の異なる署名エンジンに対する共通的なアクセス方法及びシステム及び複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体に係り、特に、平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける、署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複

5

数の異なる署名エンジンに対する共通的なアクセス方法及びシステム及び複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】最初に電子署名生成の流れと署名エンジンについて説明する。公開鍵暗号方式を用いた電子署名は、通常、図１１に示すように、まず、署名したい対象データをハッシュ関数に入れてハッシュデータに変換し、このハッシュデータに対して秘密鍵を用いた署名生成処理を行うことにより生成される。ハッシュ関数には、ＳＨＡ－１やＭＤ５などのアルゴリズムが、また、電子署名アルゴリズムには、公開鍵暗号方式であるＥＳＩＧＮやＲＳＡなどがよく知られている。ここで、電子署名に用いる秘密鍵は、署名者を識別するための情報として非常に重要な情報であるため、電子署名を利用するシステムでは、秘密鍵の管理及び電子署名の生成を安全に行うために、これらに必要な機能群をシステムと独立した専用装置として用意する場合が多い。この専用装置を一般に署名エンジンと呼んでおり、その実装方法は装置毎に様々である。

【０００３】例えば、図１１に示すように、ハッシュ処理や署名生成処理で複数のアルゴリズムを利用できるものや、複数の秘密鍵を保持及び利用できるもの、あるいは、図１１における署名エンジンＢのようにハッシュ処理部が無く、ハッシュ化されたデータが入力されることを前提とした装置も存在する。次に、署名エンジンを用いた電子署名の生成について説明する。

【０００４】一般に、複数の署名アルゴリズムの利用や複数の署名エンジンの利用を必要とするシステムにおいて電子署名を生成する際には、図１２に示すような流れで署名エンジンへの署名を生成する。

ステップ１０）　まず、署名生成を行いたいアプリケーションにおいて、署名生成に必要な情報として、署名対象となるデータ、署名生成に用いる秘密鍵、ハッシュアルゴリズム、署名アルゴリズムに何を用いるかを決定する。

【０００５】ステップ１１）　署名生成に用いる秘密鍵が格納されている署名エンジンを選択する。

ステップ１２）　選択された署名エンジンに対して、署名対象データのハッシュ化が必要か否を判断し、必要な場合にはステップ１３に移行し、不要な場合にはステップ１４に移行する。

【０００６】ステップ１３）　必要な場合には入力データのハッシュ化処理を行う。

ステップ１４）　ステップ１１で選択された署名エンジンに依存した署名生成依頼方式に従って、ステップ１０で決定された情報を元にハッシュアルゴリズム、署名アルゴリズム、秘密鍵の格納先の情報を署名エンジンへ指定するための署名生成依頼情報を生成する。ステップ１３を行った場合には、ハッシュアルゴリズムの指定は不要である。

6

【０００７】ステップ１５）　ステップ１４で生成した情報と署名対象データ、あるいは、署名対象データのハッシュ値をアクセスモジュールを介して署名エンジンへ送付し、署名エンジンから署名生成結果である署名データを受け取る。ここでアクセスモジュールとは、例えば、署名エンジンを制御するためのドライバソフトのようなものである。

【０００８】

【発明が解決しようとする課題】しかしながら、従来の署名エンジンを用いた署名生成処理では、署名生成を依頼する上位のアプリケーションが、署名生成に用いる秘密鍵が格納されている署名エンジン及びその格納場所の判別や、その秘密鍵が署名アルゴリズムに適用可能であることの確認、入力データである署名対象データのハッシュ化の要否判断などを行い、署名エンジンの種別に応じた署名生成処理の振り分けを行う必要がある。従って、用途に応じて複数の署名アルゴリズムや複数の秘密鍵、あるいは、複数の署名エンジンの使い分けを行うシステムにおいては、署名エンジンに対する電子署名の生成依頼処理が煩雑となる。

【０００９】本発明は、上記の点に鑑みなされたもので、複数の署名エンジン及び複数の署名アルゴリズムを容易に使い分けることを可能とし、また、既存のシステムへの新たな署名エンジンの追加や新たな署名アルゴリズムの追加の際にも、上位のアプリケーションに影響を与えることなく容易に追加を行うことが可能な複数の異なる署名エンジンに対する共通的なアクセス方法及びシステム及び複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。本発明（請求項１）は、平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセス方法において、複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成し（ステップ１）、署名エンジンに依存した署名エンジン依存情報を登録し、管理し（ステップ２）、署名エンジンへのアクセス依頼を受け付け（ステップ３）、指定された鍵名称を取得し（ステップ４）、秘密鍵管理テーブルから鍵名称に対応する鍵対生成または、署名作成に必要な情報を取得し（ステップ５）、任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼する（ステップ６）。

【００１１】本発明（請求項２）は、秘密鍵管理テーブ

ルから、鍵名称に対応する署名作成に必要な情報として、鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得し、取得した署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を署名エンジン依存情報から取得し、ハッシュ化が必要な場合には、秘密管理テーブルから取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して署名エンジンへ送付し、署名生成依頼を行う。

【００１２】本発明（請求項３）は、鍵対を生成する際に、利用者が指定した鍵名称を取得し、秘密鍵管理テーブルから鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得し、取得した署名エンジン種別に対応するアクセスモジュール種別情報を署名エンジン依存情報から取得し、鍵格納場所、署名アルゴリズム、及び鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼し、署名エンジンにおいて、依頼された鍵対を生成する。

【００１３】本発明（請求項４）は、利用者が指定する鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを秘密鍵管理テーブルに保持する。

【００１４】図２は、本発明の原理構成図である。本発明（請求項５）は、平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセスシステムであって、複数の秘密鍵の管理や複数の電子署名アルゴリズムの利用が可能な任意の数の電子署名エンジン２００と、複数の秘密鍵情報を管理する秘密鍵管理テーブル１５０を作成する秘密鍵管理テーブル作成手段１１０と、署名エンジンに依存した情報である署名エンジン依存情報を登録し、管理する署名エンジン依存情報登録手段１３０と、署名エンジン２００へのアクセス依頼を受け付け、指定された鍵名称を取得する署名エンジンアクセス依頼受付手段１２０と、秘密鍵管理テーブル１５０から鍵名称に対応する秘密鍵情報及び、署名作成に必要な情報を取得する秘密鍵情報参照手段１４０と、任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼する署名エンジンアクセス制御手段１６０とを有する。

【００１５】本発明（請求項１０）は、秘密鍵情報参照手段１４０において、秘密鍵管理テーブル１５０から、鍵名称に対応する署名作成に必要な情報として、該鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得する手段を有し、署名エンジンアクセス制御手段１６０において、取得した署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を署名エンジン依存情報から取得する手段と、ハッシュ化が必要な場合には、秘密管理テーブル１５０から取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して署名エンジンへ送付し、署名生成依頼を行う手段を有する。

【００１６】本発明（請求項１１）は、利用者が指定した鍵名称を取得する手段と、秘密鍵管理テーブル１５０から鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得する手段と、取得した署名エンジン種別に対応するアクセスモジュール種別情報を署名エンジン依存情報から取得する手段と、鍵格納場所、署名アルゴリズム、及び鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼する手段とを有する鍵対生成依頼手段を更に有し、署名エンジンにおいて、依頼された鍵対を生成する。

【００１７】本発明（請求項８）は、秘密鍵管理テーブル１５０において、利用者が指定する鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを保持する。

【００１８】本発明（請求項９）は、平文または、平文のダイジェストに対して公開鍵暗号技術を用いた電子署名を作成するための電子署名エンジンを有する情報処理システムにおける署名エンジンを用いた電子署名の生成及び、秘密鍵／公開鍵の鍵対の生成を行う複数の異なる署名エンジンに対する共通的なアクセスプログラムを格納した記憶媒体であって、複数の秘密鍵情報を管理する秘密鍵管理テーブルを作成する秘密鍵管理テーブル作成プロセスと、複数の秘密鍵の管理や複数の電子署名アルゴリズムの利用が可能な任意の数の電子署名エンジンに依存した情報である署名エンジン依存情報を登録し、管理する署名エンジン依存情報登録プロセスと、署名エンジンへのアクセス依頼を受け付け、指定された鍵名称を取得する署名エンジンアクセス依頼受付プロセスと、秘密鍵管理テーブルから鍵名称に対応する秘密鍵情報及

び、署名作成に必要な情報を取得する秘密鍵情報参照プロセスと、任意の署名エンジンに対して鍵対生成処理または、署名生成処理を依頼する署名エンジンアクセス制御プロセスとを有する。

【００１９】本発明（請求項１０）は、秘密鍵情報参照プロセスにおいて、秘密鍵管理テーブルから、鍵名称に対応する署名作成に必要な情報として、該鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズムの署名生成に必要な情報を取得するプロセスを有し、署名エンジンアクセス制御プロセスにおいて、取得した署名エンジン種別情報に対応するアクセスモジュール種別と入力データのハッシュ化の要否情報を署名エンジン依存情報から取得するプロセスと、ハッシュ化が必要な場合には、秘密管理テーブルから取得したハッシュアルゴリズムによる署名対象データのハッシュデータ及び鍵格納場所、及び署名アルゴリズム情報を、ハッシュ化が不要な場合には、署名対象データ、鍵格納場所、及び署名アルゴリズム及びハッシュアルゴリズム情報を、選択されたアクセスモジュールを介して署名エンジンへ送付し、署名生成依頼を行うプロセスを有する。

【００２０】本発明（請求項１１）は、利用者が指定した鍵名称を取得するプロセスと、秘密鍵管理テーブルから鍵名称に対応付けられた署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータの鍵対生成に必要な情報を取得するプロセスと、取得した署名エンジン種別に対応するアクセスモジュール種別情報を署名エンジン依存情報から取得するプロセスと、鍵格納場所、署名アルゴリズム、及び鍵パラメータを選択されたアクセスモジュールを介して署名エンジンへ送付し、鍵対生成を依頼するプロセスとを有する鍵対生成依頼プロセスを更に有する。

【００２１】本発明（請求項１２）は、利用者が指定する鍵名称に対して、該鍵名称に対応する秘密鍵が格納されている署名エンジン種別と、鍵格納場所と、秘密鍵が適用される署名アルゴリズムと、鍵長を含む鍵パラメータ情報と、署名生成時に署名対象データをハッシュ化するためのハッシュアルゴリズム種別とを保持する秘密鍵管理テーブルを利用するプロセスを有する。

【００２２】上記のように、本発明において、初期設定時における秘密鍵管理テーブルの設定により、上位アプリケーションは、署名生成に用いる秘密鍵の鍵名称のみを指定するだけで、任意の署名エンジンに対する署名生成や鍵対生成の依頼に必要な情報を決定可能になる。また、署名エンジン依存情報の登録を行うことにより、署名エンジンに依存した情報を秘密鍵制御部内に隠蔽し、上位アプリケーションが署名エンジンの種別を意識せずに署名エンジンへアクセスすることが可能となる。

【００２３】また、鍵対生成処理により、秘密鍵の格納先や署名アルゴリズム等に関わらず、システムが利用するすべての秘密鍵の情報を一元的に管理して、各秘密鍵の生成やその秘密鍵を用いた署名生成に必要な情報を、鍵名称をキー情報として取得することが可能となる。また、署名生成に用いる秘密鍵の生成の際にも、上位アプリケーションが生成したい秘密鍵の鍵名称のみを指定するだけで、任意の署名エンジンに対する鍵対生成依頼が可能になる。

【００２４】また、署名生成処理により、上位のアプリケーションが署名生成処理を署名エンジンに依頼する際に、秘密鍵の格納場所や、署名アルゴリズム、利用する署名エンジンの種別及びその署名エンジンに応じた処理依頼方法などを意識することなく、鍵名称及び署名対象データを指定するだけで署名エンジンへの署名生成依頼が可能となる。

【００２５】

【発明の実施の形態】図３は、本発明におけるアクセスシステム構成を示す。同図に示すように、複数の秘密鍵の管理や複数の署名エンジンへのアクセス制御を一元的に行うための秘密鍵制御部１００を設け、署名生成を依頼する上位アプリケーション４００が、秘密鍵の格納先や、格納先にある秘密鍵の署名アルゴリズムへの適用性や、入力データのハッシュ化の要否判断などを意識することなく、この秘密鍵制御部１００に対して署名生成に用いる秘密鍵名称を指定するだけで任意の署名エンジンに対する署名生成依頼が可能となる。

【００２６】秘密鍵制御部１００は、上位アプリケーション４００から署名エンジン（Ａ２００または、Ｂ３００）へのアクセス依頼を受け付けるための署名エンジンアクセス依頼受付部１２０と、システムが利用する複数の秘密鍵の各々について、格納先や署名アルゴリズムなどの署名生成に必要な情報を管理するための秘密鍵管理テーブル１５０、及びその生成を行う秘密鍵管理テーブル作成部１１０、この秘密鍵管理テーブル１５０から鍵名称をキー情報として対応する署名生成に必要な情報を取得するための秘密鍵情報参照部１４０、署名エンジンに依存した情報を予め登録しておくための署名エンジン依存情報登録部１３０と、秘密鍵が格納されている署名エンジンへアクセスモジュール１７０、１８０を介して実際の処理依頼を行うための署名エンジンアクセス制御部１６０から構成される。

【００２７】次に、本発明の動作を説明する。最初に、署名生成を実現するために必要な事前処理として、秘密鍵情報を一元管理するための秘密鍵管理テーブル１５０の設定及び署名エンジンに依存した情報の設定と、署名生成に用いる秘密鍵を用意するための鍵対生成処理について説明する。

【００２８】１．システム初期設定時

図４は、本発明における鍵対生成時の処理の流れを説明するための図であり、図５は、本発明の秘密鍵管理テーブルの例を示す。最初にシステム初期設定時における動

作を説明する。

（１）　秘密鍵管理テーブル１５０の設定（ステップ１０１）：システム初期設定の際に、図５に示すように、上位アプリケーション４００が利用する複数の秘密鍵の各々に対して、鍵名称、鍵名称に対応する秘密鍵が格納されている署名エンジン種別及びその中における格納場所を示す鍵格納場所情報、適用する署名アルゴリズム情報、署名生成処理の前に署名対象データをハッシュ化するためのハッシュアルゴリズム情報、鍵長などの鍵対生成に必要な鍵パラメータ情報を管理する秘密鍵管理テーブル１５０を、秘密鍵管理テーブル作成部１１０を用いて作成する。

【００２９】ここで、署名エンジン種別とは、署名エンジンの種類を区別するための識別子のことであり、署名エンジンとこの識別子との対応はシステムとして固定的に保持する情報である。これらの情報は、署名エンジンに対する鍵対生成や署名生成を依頼する際に必要な情報であり、このテーブルに上位アプリケーション４００が利用するすべての秘密鍵に関する情報を設定することにより、上位アプリケーション４００は、署名生成に用いる秘密鍵の鍵名称のみを指定するだけで、任意の署名エンジンに対する署名生成や鍵対生成の依頼に必要な情報を決定可能になる。

【００３０】（２）　署名エンジン依存情報の登録（ステップ１０２）：システムの初期設定の際に、システムが利用する各署名エンジンに依存する情報として、署名生成を依頼する際の入力データとして署名対象データをハッシュ化する必要があるか否かの情報と、署名エンジンンへアクセスするためのアクセスモジュール種別を秘密鍵制御部１００内に予め登録しておく。これにより、署名エンジンに依存した情報を秘密鍵制御部１００内に隠蔽し、上位アプリケーション４００が署名エンジンの種別を意識せずに署名エンジンへアクセスすることが可能となる。ここで、アクセスモジュール種別とは、アクセスモジュールの種別を区別するための識別子のことであり、アクセスモジュールと識別子の対応は、システムとして固定的に保持される情報である。

【００３１】２．鍵生成時

次に、鍵対生成時の動作について説明する。

（１）　上位アプリケーション４００による鍵対生成依頼（ステップ１０３）：上記システム初期時の設定が終了後、上位アプリケーション４００は署名生成に用いる鍵対の生成処理を秘密鍵制御部１５０に対して依頼する。その際、上位アプリケーション４００は、どの鍵対を生成するのかを先に作成した秘密鍵管理テーブル１５０内に登録した秘密鍵の中から鍵名称を用いて指定する。

【００３２】（２）　署名エンジンアクセス依頼受付処理（ステップ１０４）：上位アプリケーション４００から署名エンジンに対する鍵対生成の依頼を、署名エンジンアクセス依頼受付部１２０を用いて受理し、生成依頼対象である鍵名称情報を取得する。

（３）　秘密鍵情報参照処理（ステップ１０５）：上位アプリケーション４００から指定された鍵名称に対応する鍵対の生成に必要な情報を取得するため、秘密鍵情報参照部１４０を用いて秘密鍵管理テーブル１５０にアクセスし、（２）で取得した鍵名称をキー情報として対応する署名エンジン種別、鍵格納場所、署名アルゴリズム、鍵パラメータ情報を取得する。これにより、上位アプリケーション４００からは鍵名称のみが指定されるだけで、署名エンジンへの鍵対生成の依頼に必要な情報を用意することが可能となる。

【００３３】（４）　署名エンジンへの鍵対生成依頼処理（ステップ１０６）：

（３）で取得した情報をもとに署名エンジンへ鍵対生成処理を依頼するため、署名エンジンアクセス制御部１００を用いて、（３）で取得した署名エンジン種別に対応する署名エンジンへのアクセスモジュール種別を署名エンジン依存情報から取得し、そのアクセスモジュールを介して、（３）で取得した鍵格納場所、署名アルゴリズム、鍵パラメータ情報を用いて署名エンジンに対して鍵対生成を依頼する。この処理により、上位アプリケーション４００が指定した鍵名称に対応する秘密鍵が生成・格納されるべき署名エンジンへのアクセスモジュールが自動的に選択され、各署名エンジンにおける鍵対生成依頼方法に従った鍵対生成依頼を実行することが可能となる。

【００３４】（５）　鍵対生成処理（ステップ１０７）：（４）の依頼に基づき、指定された鍵パラメータ及び署名アルゴリズムに対応する鍵対生成処理が署名エンジン内で行われ、指定された格納場所へ秘密鍵が格納される。以上の処理及び機能を用いることにより、秘密鍵の格納先や署名アルゴリズム等に関わらず、システムが利用するすべての秘密鍵の情報を一元的に管理して、各秘密鍵の生成やその秘密鍵を用いた署名生成に必要な情報を、鍵名称をキー情報として取得することが可能となる。また、本発明により、署名生成に用いる秘密鍵の生成の際にも、上位アプリケーション４００が生成したい秘密鍵の鍵名称のみを指定するだけで、任意の署名エンジンに対する鍵対生成依頼が可能になる。

【００３５】３．署名生成処理時次に、上記で生成された秘密鍵を用いた署名生成処理の流れについて説明する。図６は、本発明における署名生成処理の流れを説明するための図である。最初に、署名生成処理時の動作について説明する。

（１）　上位アプリケーション４００による署名生成依頼（ステップ２０１）：上位アプリケーション４００は、署名生成の必要が発生した際に、秘密鍵制御部１５０に対して署名対象となるデータと署名に用いる鍵名称を指定して署名生成依頼を行う。

13

【００３６】（２）　署名生成依頼受付処理（ステップ２０２）：上位アプリケーション４００から署名エンジンに対する署名生成の依頼を、署名エンジンアクセス依頼受付部１２０を用いて受理し、署名対象となるデータと署名に用いる秘密鍵の鍵名称情報を取得する。

（３）　秘密鍵情報参照処理（ステップ２０３）：上位アプリケーション４００から指定された鍵名称に対応する秘密鍵を用いた署名生成に必要な情報を取得するため、秘密鍵情報参照部１４０を用いて秘密鍵管理テーブル１５０にアクセスし、（２）で取得した鍵名称をキー情報として対応する署名エンジン種別、鍵格納場所、署名アルゴリズム、ハッシュアルゴリズム情報を取得する。これにより、上位アプリケーション４００からは鍵名称のみが指定されるだけで、署名エンジンへの署名生成の依頼に必要な情報を用意することが可能になる。

【００３７】（４）　署名エンジンへの署名生成依頼処理（ステップ２０４）：（３）で取得した情報をもとに署名エンジンへの署名生成処理を依頼するため、署名エンジンアクセス制御部１６０を用いて、（３）で取得した署名エンジン種別に対応する署名エンジンへのアクセスモジュール種別及び署名対象データのハッシュ化要否情報を署名エンジン依存情報から取得する。そして、選択された署名アクセスモジュールに対して、署名対象のデータのハッシュ化が必要であった場合には、（３）で取得したハッシュアルゴリズムにより入力データである署名対象データをハッシュ化後、このハッシュデータと鍵格納場所と署名アルゴリズムの情報を入力として署名エンジンへの署名生成依頼を行い、署名対象データのハッシュ化が不要であった場合には、署名対象データと、（３）で取得した鍵格納場所及び署名アルゴリズム及びハッシュアルゴリズム情報を入力として署名エンジンへ署名生成依頼を行う。この処理により、上位アプリケーション４００が指定した鍵名称に対応する秘密鍵が格納されている署名エンジンへのアクセスモジュールが自動的に選択され、入力データのハッシュ化の要否など各署名エンジンに対する署名生成依頼方法に従った署名生成依頼を実行することが可能となる。

【００３８】（５）　署名生成処理（ステップ２０５）：署名エンジンにおいて、（４）の依頼に基づき、指定された鍵格納場所にある秘密鍵を用いて署名生成処理が行われ、署名データが返却される。以上の処理及び機能を用いることにより、上位アプリケーション４００が署名生成処理を署名エンジンに依頼する際に、秘密鍵の格納場所や、署名アルゴリズム、利用する署名エンジンの種別及びその署名エンジンに応じた処理依頼方法などを意識することなく、鍵名称及び署名対象データを指定するだけで署名エンジンへの署名生成依頼が可能となる。

【００３９】

【実施例】以下、図面と共に本発明の実施例を説明する。本実施例では、署名エンジンを用いた署名生成処理の流れを図７～図１０を用いて説明する。図７は、本発明の一実施例の電子署名生成の事前処理を説明するための図であり、図８は、本発明の一実施例の秘密鍵管理テーブルの設定例を示す。

14

【００４０】１．　システム処刑設定時

（１）　秘密鍵管理テーブルの設定（ステップ３０１）：システム初期設定の際に、図８の例に示されるような秘密鍵管理テーブル１５０を作成し、その中にシステムで利用されるすべての秘密鍵について、署名エンジンへの鍵対生成や署名生成の依頼に必要な情報を登録する。このようなテーブルの作成は、例えば、ファイル編集機能を用いて実現可能である。また、図８は、例えば、「ＫｅｙＡ」という鍵名称を持つ秘密鍵が、「署名エンジンＡ」２００の「＃３」という場所に格納され、適用する署名アルゴリズムは「ＥＳＩＧＮ」であり、署名生成の際の署名対象データのハッシュ化アルゴリズムには「ＳＨＡ－１」を用い、鍵長が「１２０バイト」であるといった情報が登録されている。これらの情報は、システム初期時にシステムの方針として予め決定しておく。

【００４１】（２）　署名エンジン依存情報の登録（ステップ３０２）：図９は、本発明の一実施例の署名エンジン依存情報の設定例を示す。システム初期設定の際に、図９の例に示されるような署名エンジン依存情報テーブル１６１を署名エンジンアクセス制御部１６０に作成し、その中にシステムが利用する署名エンジンに対して、署名エンジンに依存する情報である入力データのハッシュ化の要否情報と、署名エンジンへアクセスするためのアクセスモジュール種別情報を登録する。このようなテーブルの作成は、例えば、ファイル編集機能を用いて実現可能である。また、図９は、例えば、「署名エンジンＡ」２００は、入力データのハッシュ化の要否は「否」であり、署名エンジンにアクセスする際に使用するアクセスモジュールは、「アクセスモジュールＡ」を使用することを意味している。これらの情報は、システム初期時に予め使用する署名エンジンの仕様を調査して取得しておく。

【００４２】２．　鍵対生成時

（１）　上位アプリケーション４００による鍵対生成依頼（ステップ３０３）：上記システム初期時の設定が終了後、上位アプリケーションは署名生成に用いる鍵対の生成処理を秘密鍵制御部１００に対して鍵名称を指定して依頼する。本実施例では、上位アプリケーション４００が「ＫｅｙＡ」の鍵名称に対応する鍵の生成を依頼したものとして説明する。

【００４３】（２）　署名エンジンアクセス依頼受付処理（ステップ３０４）：上位アプリケーション４００から署名エンジンに対する鍵対生成の依頼を受理し、生成依頼対象が鍵名称「ＫｅｙＡ」であることを認識する。

上位アプリケーション４００からの依頼の受理は、例えば、データ通信機能を用いて実現可能であり、依頼内容を解析し、鍵名称情報を取得することは、例えば、データ解析機能を用いて実現可能である。

【００４４】（３）　秘密鍵情報参照処理（ステップ３０５）：上位アプリケーション４００から指定さた「ＫｅｙＡ」に対応する鍵対の生成に必要な情報を取得するため、秘密鍵管理テーブル１５０のファイルにアクセスし、「ＫｅｙＡ」に対応する情報として、署名エンジン種別が「署名エンジンＡ」であり、鍵格納場所が「＃３」であり、署名アルゴリズムが「ＥＳＩＧＮ」であり、鍵パラメータとして秘密鍵の鍵長が「４０バイト」であることの情報を取得する。秘密鍵管理テーブル１５０のファイルへのアクセスは、例えば、ファイルアクセス機能を用いて実現可能であり、「ＫｅｙＡ」に対応する情報の取得は、例えば、データ検索機能を用いて実現可能である。

【００４５】（４）　署名エンジンへの鍵対生成依頼処理（ステップ３０６）：署名エンジンへ鍵対生成処理を依頼するため、まず、初期時に設定した署名エンジン依存情報テーブル１６１から署名エンジン種別である「署名エンジンＡ」に対応するアクセスモジュール種別である「アクセスモジュールＡ」の情報を取得する。その後、この「アクセスモジュールＡ」を介して、（３）で取得した鍵格納場所「＃３」、署名アルゴリズム「ＥＳＩＧＮ」、鍵パラメータ情報「秘密鍵長＝４０バイト」の情報を「署名エンジンＡ」に対して送付し、鍵対生成を依頼する。署名エンジン依存情報テーブル１６１からのアクセスモジュール種別情報の取得は、例えば、データ検索機能を用いて実現可能であり、アクセスモジュールへの入力データの生成は、例えば、データ組み立て機能を用いて実現可能である。また、署名エンジンへの鍵対生成依頼データの送付は、例えば、データ通信機能を用いて実現される。

【００４６】（５）　鍵対生成処理（ステップ３０７）：（４）の依頼に基づき、「署名エンジンＡ」２００では、「ＥＳＩＧＮ」に適用花王で、「秘密鍵の鍵長が４０バイト」の鍵対の生成を行い、そこで生成された秘密鍵が「＃３」に格納される。以上の処理により、署名生成に用いる秘密鍵管理情報の設定及び、それに基づく秘密鍵の生成を、上位アプリケーション４００が署名エンジン種別や署名アルゴリズムなどを意識することなく実行することが可能となる。

【００４７】３．　署名生成処理時

続いて本発明における署名生成処理の例を説明する。図１０は、本発明の一実施例の署名生成処理を説明するための図である。

（１）　上位アプリケーション４００による署名生成依頼（ステップ４０１）：上位アプリケーション４００は、署名生成の必要が発生した際に、秘密鍵制御部１００に対して署名対象となるデータと署名に用いる秘密鍵の鍵名称を指定して署名生成依頼を行う。本実施例では、上位アプリケーション４００が署名生成に用いる秘密鍵として「ＫｅｙＡ」の鍵名称に対応する秘密鍵を指定して署名生成依頼を行ったものとして説明する。

【００４８】（２）　署名生成依頼受付処理（ステップ４０２）：上位アプリケーション４００から署名エンジンに対する署名生成の依頼を受理し、署名対象データと署名に用いる秘密鍵の鍵名称情報が「ＫｅｙＡ」であることを認識する。上位アプリケーション４００からの依頼の受理は、例えば、データ通信機能を用いて実現可能であり、依頼内容を解析し、鍵名称情報を取得することは、例えば、デーた解析機能を用いて実現可能である。

【００４９】（３）　秘密鍵情報参照処理（ステップ４０３）：上位アプリケーション４００から指定された「ＫｅｙＡ」に対応する鍵対の生成に必要な情報を取得するため、秘密鍵管理テーブルのファイルにアクセスし、「ＫｅｙＡ」に対応する情報として、署名エンジン種別が、「署名エンジンＡ」であり、鍵格納場所が「＃３」であり、署名アルゴリズムが「ＥＳＩＧＮ」であり、ハッシュアルゴリズムが「ＳＨＡ－１」であることの情報を取得する。秘密鍵管理テーブル１５０のファイルへのアクセスは、例えば、ファイルアクセス機能を用いて、実現可能であり、「ＫｅｙＡ」に対応する情報の取得は、例えばデータ検索機能を用いて実現可能である。

【００５０】（４）　署名エンジンへの署名生成依頼処理（ステップ４０４）：署名エンジンへ署名生成処理を依頼するため、まず、システム初期時に設定した署名エンジン依存情報テーブル１６１から署名エンジン種別である「署名エンジンＡ」に対応するアクセスモジュール種別である「アクセスモジュールＡ」と、入力データのハッシュ化の要否情報である「否」の情報を取得する。入力データのハッシュ化の要否が「否」であることを確認し、これにより入力データのハッシュ化処理は行わず、「アクセスモジュールＡ」を介して、（３）で取得した鍵格納場所「＃３」、署名アルゴリズム「ＥＳＩＧＮ」、ハッシュアルゴリズム「ＳＨＡ－１」の情報と、署名対象データを「署名エンジンＡ」に対して送付し、署名生成を依頼する。署名エンジン依存情報テーブル１６１からのアクセスモジュール種別情報及び入力データのハッシュ化要否情報の取得は、例えば、データ検索機能を用いて実現可能であり、入力データのハッシュ化処理の要否判断は、例えば、データ解析機能を用いて実現可能であり、アクセスモジュールへの入力データの生成は、例えばデータ組み立て機能を用いて実現可能であり、署名エンジンへの鍵対生成依頼データの送付は、例えば、データ通信機能を用いて実現される。また、入力データのハッシュ化の要否が「要」であった場合には、例えば、ソフトウェアで実現されているハッシュ化機能

17

を用いてハッシュ処理を行うことが可能である。

【００５１】（５）　署名生成処理（ステップ４０５）：（４）の依頼に基づき、「署名エンジンＡ」２００では、署名対象データを指定さたハッシュアルゴリズムである「ＳＨＡ－１」によりハッシュ化し、これに対して「＃３」に格納されている秘密鍵を用いて「ＥＳＩＧＮ」署名アルゴリズムにより暗号化し、署名が生成される。

【００５２】以上の処理により、上位アプリケーションが署名生成処理を署名エンジンに依頼する際に、鍵名称及び署名対象データを秘密鍵管理テーブル１５０に対して指定するだけで、任意の署名エンジンに対して署名生成の依頼が可能になる。また、上記の実施例は、図３の構成に基づいて説明したが、秘密鍵管理テーブル作成部１１０、署名エンジンアクセス依頼受付部１２０、署名エンジン依存情報登録部１３０、秘密鍵情報参照部１４０、署名エンジンアクセス制御部１６０を有する秘密鍵制御部１００をプログラムとして構築し、秘密鍵制御部として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【００５３】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【００５４】

【発明の効果】上述のように、本発明によれば、上位アプリケーションは署名生成のためにアクセスする署名エンジンの種別、秘密鍵の格納場所、署名アルゴリズムなどを意識することなく、鍵名称と署名対象データのみという統一的なインタフェースにより、任意の署名エンジンに対して電子署名の生成を依頼することが可能となるため、複数の署名エンジン及び複数の署名アルゴリズムを容易に使い分けることが可能となることはもちろん、既存システムへの新たな署名エンジンの追加や新たな署名アルゴリズムの追加の際にも、上位のアプリケーションに影響を与えることなく、容易に追加を行うことができる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明におけるアクセスシステムの構成図である。

18

【図４】本発明における鍵対生成時の処理の流れを説明するための図である。

【図５】本発明の秘密鍵管理テーブルの例である。

【図６】本発明における署名生成処理の流れを説明するための図である。

【図７】本発明の一実施例の署名生成のための事前処理を説明するための図である。

【図８】本発明の一実施例の秘密鍵管理テーブルの設定例である。

【図９】本発明の一実施例の署名エンジン依存情報の設定例である。

【図１０】本発明の一実施例の署名生成処理を説明するための図である。

【図１１】電子署名生成の流れと署名エンジンの構成図である。

【図１２】従来の署名エンジンへの署名生成依頼処理の流れを説明するための図である。

【符号の説明】

１００　秘密鍵制御部

１１０　秘密鍵管理テーブル作成手段、秘密鍵管理テーブル作成部

１２０　署名エンジンアクセス依頼受付手段、署名エンジンアクセス依頼受付部

１３０　署名エンジン依存情報登録手段、署名エンジン依存情報登録部

１４０　秘密鍵情報参照手段、秘密鍵情報参照部

１５０　秘密鍵管理テーブル

１６０　署名エンジンアクセス制御手段、署名エンジンアクセス制御部

１６１　署名エンジン依存情報

１７０　署名アクセスモジュールＡ

１８０　署名アクセスモジュールＢ

２００　署名エンジン、署名エンジンＡ

２１０　ハッシュ処理部

２２０　署名生成部

２３０　秘密鍵格納部

２４０　鍵対生成部

３００　署名エンジンＢ

３２０　署名生成部

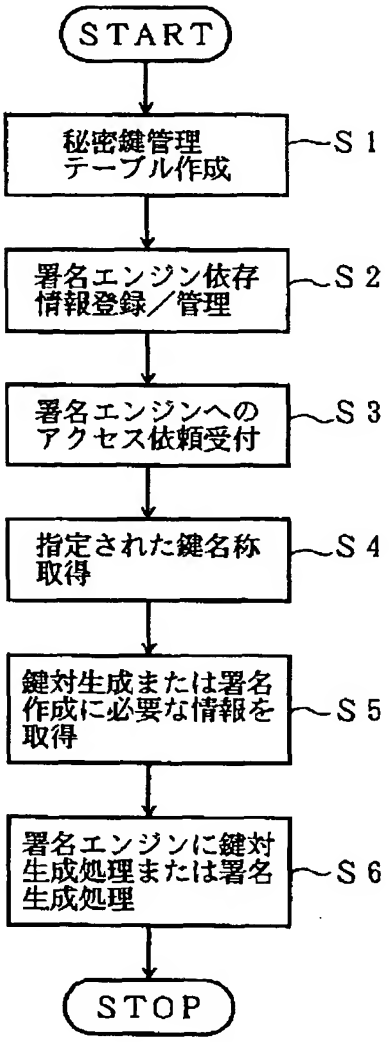
３３０　秘密鍵格納部

３４０　鍵対生成部

４００　上位アプリケーション

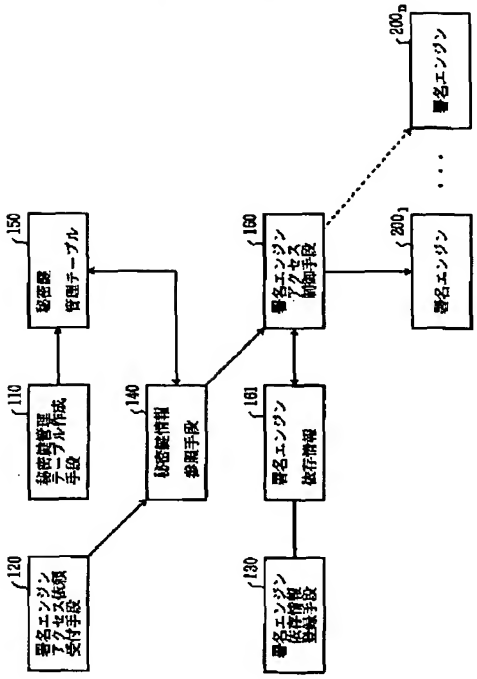
【図１】

本発明の原理を説明するための図



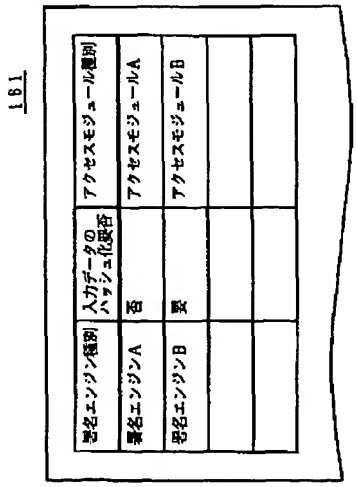
【図２】

本発明の原理構成図



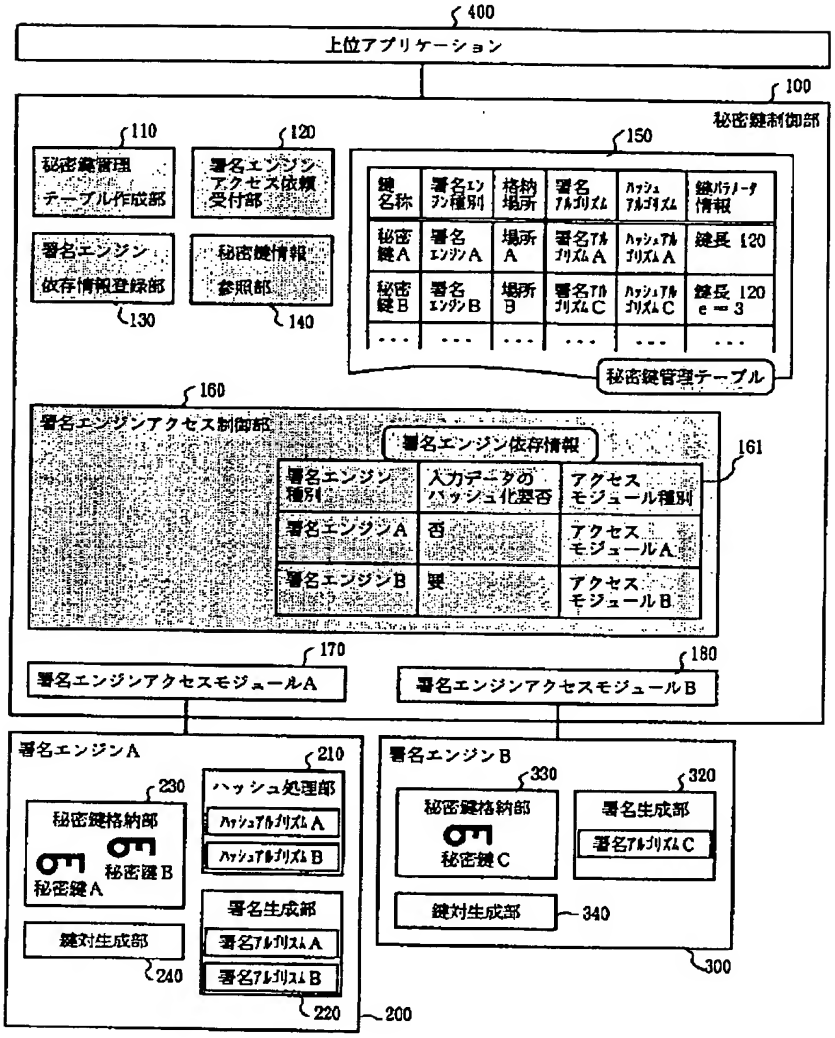
【図９】

本発明の一実施例の署名エンジン依存情報の設定例



【図３】

本発明におけるアクセスシステム構成図



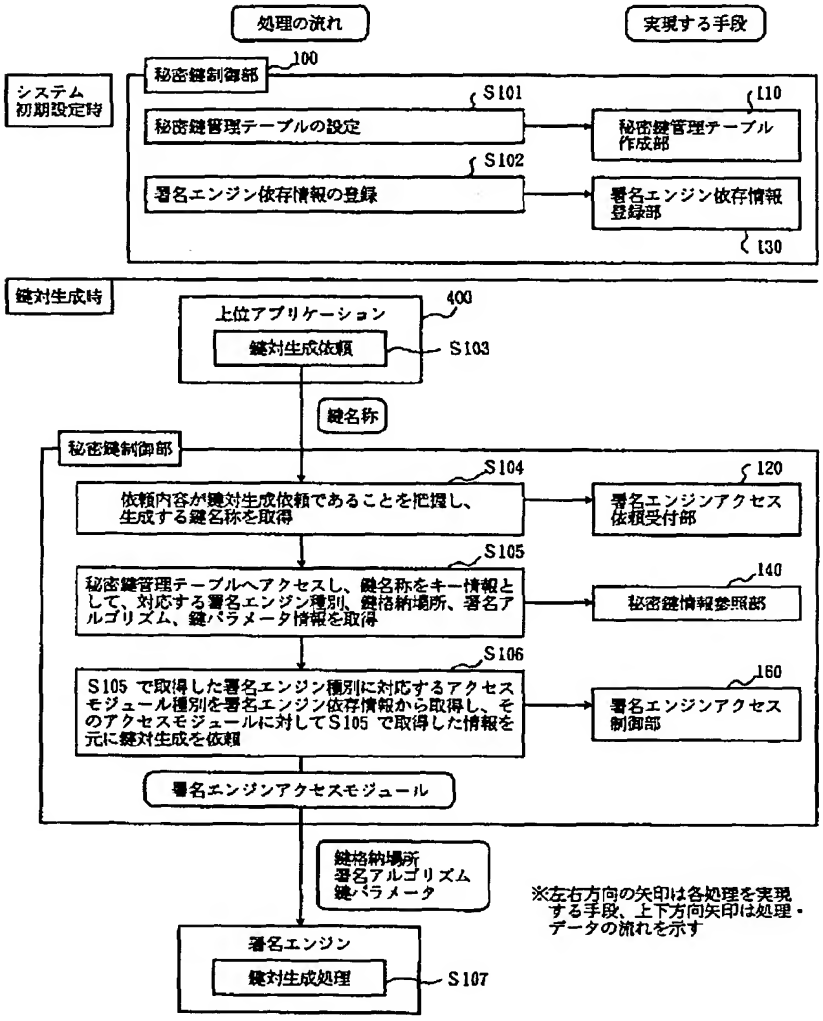
【図５】

本発明の秘密鍵管理テーブルの例

鍵名称	署名エンジン種別	格納場所	署名アルゴリズム	ハッシュアルゴリズム	鍵パラメータ情報		
秘密鍵A	署名エンジンA	場所A	署名アルゴリズムA	ハッシュアルゴリズムA	鍵長 120		
秘密鍵B	署名エンジンB	場所B	署名アルゴリズムC	ハッシュアルゴリズムC	鍵長 120 e＝3		
・・・	・・・	・・・	・・・	・・・	・・・		

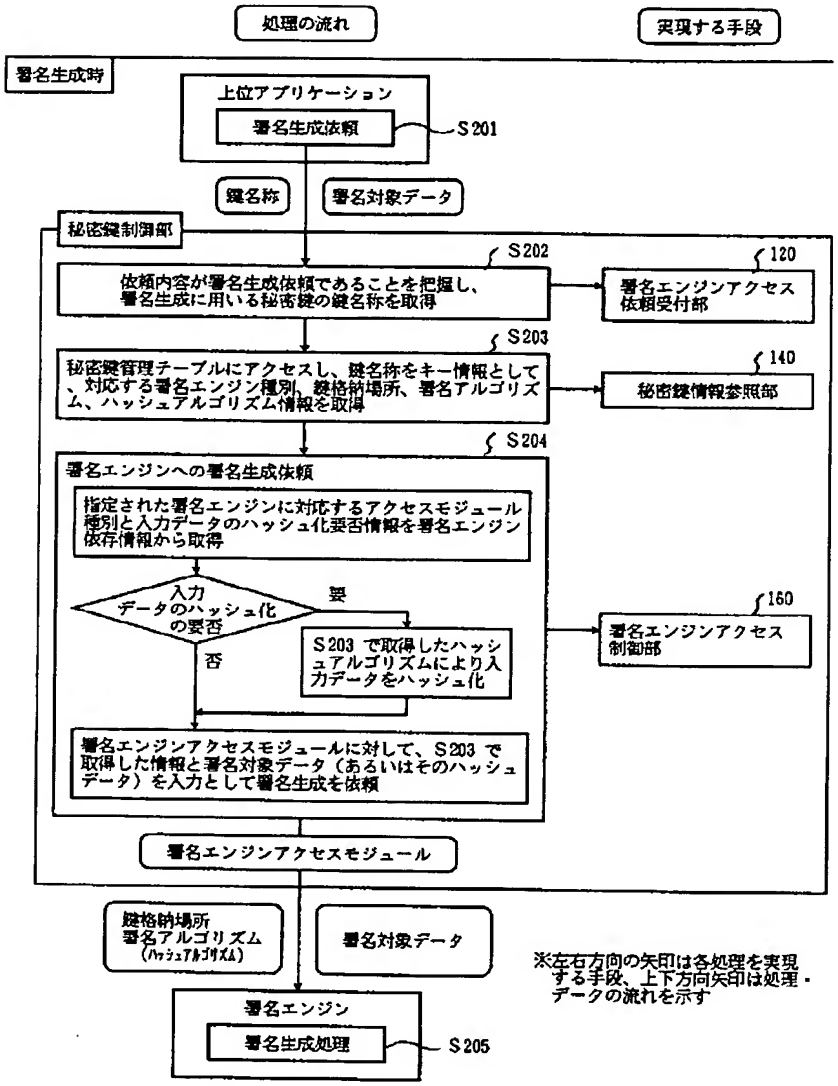
【図４】

本発明における鍵対生成時の処理の流れを説明するための図



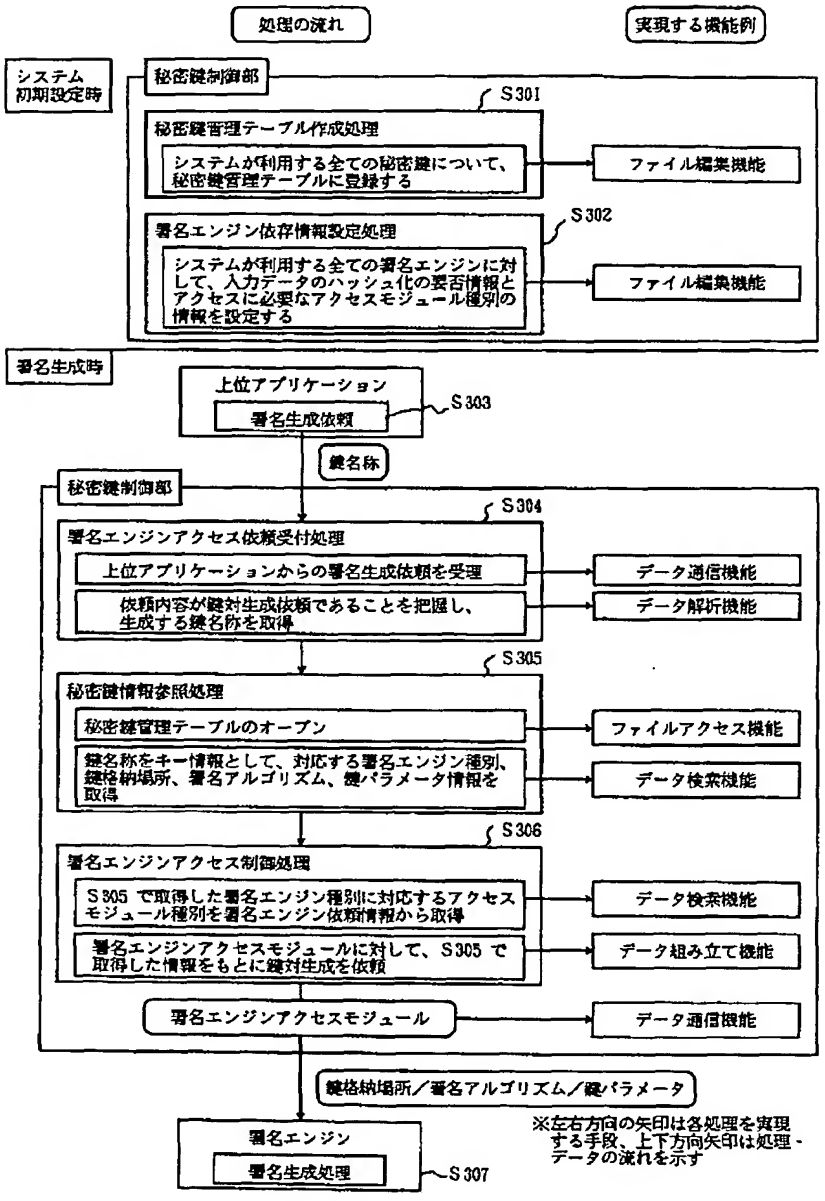
【図６】

本発明における署名生成処理の流れを説明するための図



【図７】

本発明の一実施例の署名生成のための事前処理を説明するための図



【図８】

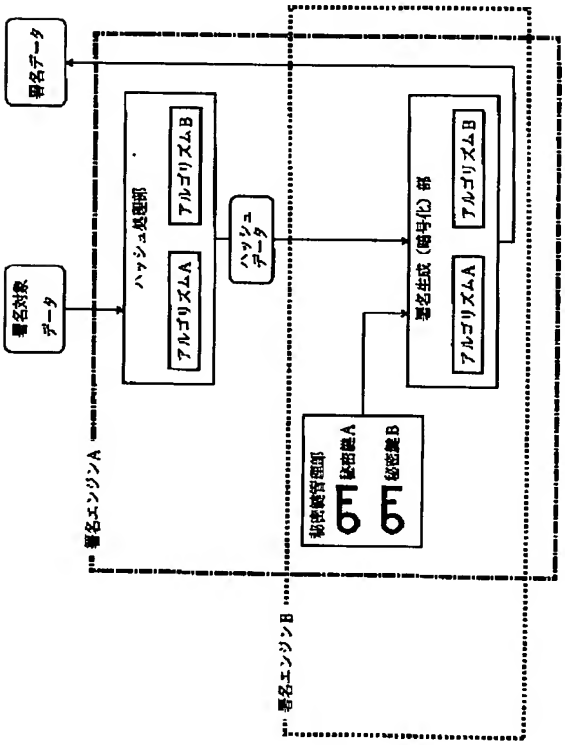
本発明の一実施例の秘密鍵管理テーブルの設定例

150

鍵名称	署名エンジン種別	格納場所	署名アルゴリズム	ハッシュアルゴリズム	鍵パラメータ情報
KeyA	署名エンジンA	#3	BSIGN	SHA-1	鍵長 120
KeyB	署名エンジンB	/key/keyB.dat	RSA	MD5	鍵長 128 e=3

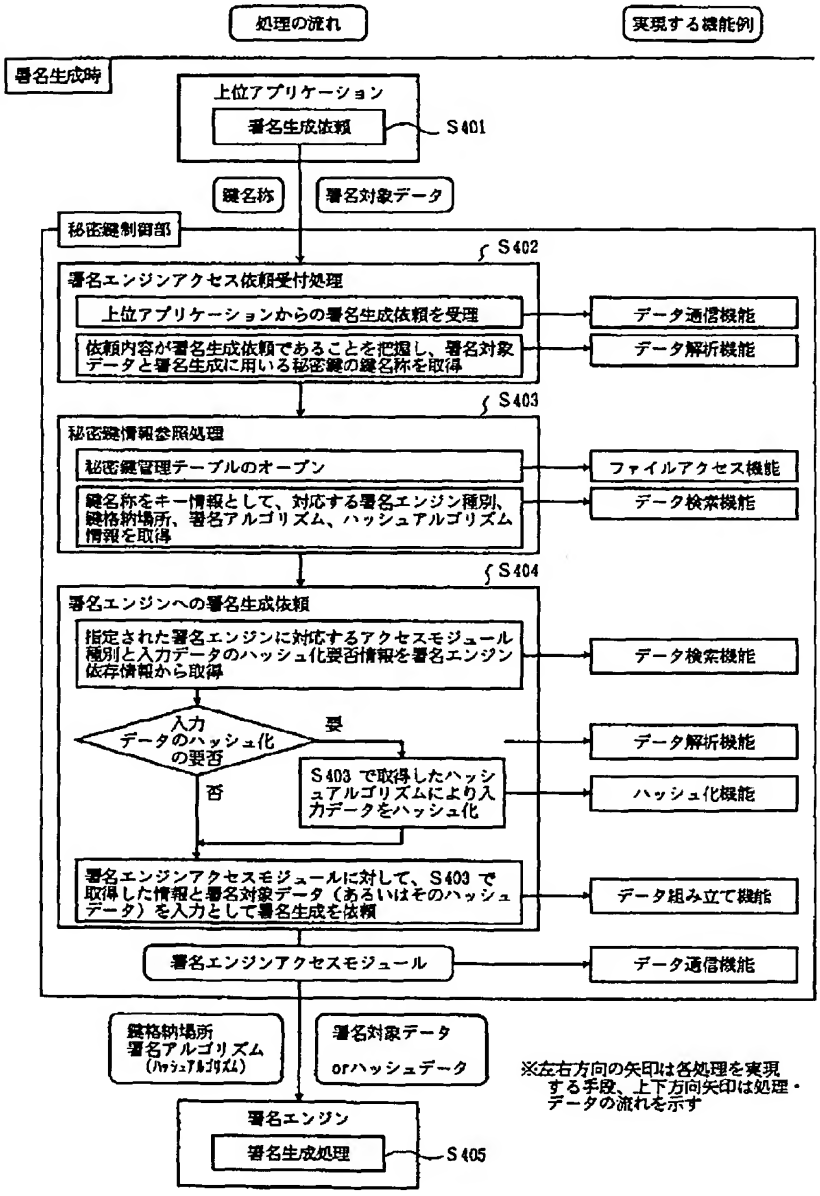
【図１１】

電子署名生成の流れと署名エンジンの構成図



【図１０】

本発明の一実施例の署名生成処理を説明するための図



【図１２】

従来の署名エンジンへの署名生成依頼処理の流れを説明するための図